

by ensuring that such information is expeditiously and securely shared with appropriate authorities including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to assist in preventing, preempting, and disrupting terrorist threats to our homeland. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

- (1) The acknowledgement of receipt by DHS of voluntarily submitted CII;
- (2) The maintenance of the identification of CII voluntarily submitted to DHS for purposes of, and subject to the provisions of the CII Act of 2002;
- (3) The receipt, handling, storage, and proper marking of information as Protected CII;
- (4) The safeguarding and maintenance of the confidentiality of such information that permits the sharing of such information within the Federal government and with foreign, State, and local governments and government authorities, and the private sector or the general public, in the form of advisories or warnings; and
- (5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner as to protect from unauthorized disclosure the identity of the submitting person or entity as well as information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily available in the public domain.

(b) *Scope.* These procedures apply to all Federal agencies that handle, use, or store Protected CII pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to foreign, State, and local governments, and to government authorities, pursuant to any necessary express written agreements, treaties, bilateral agreements, or other statutory authority.

§ 29.2 Definitions.

For purposes of this part:

Critical Infrastructure has the definition referenced in section 2 of the Homeland Security Act of 2002 and

means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning:

- (1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety;
- (2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or
- (3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Critical Infrastructure Information Program, or CII Program means the maintenance, management, and review of these procedures and of the information provided to DHS in furtherance of the protections provided by the CII Act of 2002.

Information Sharing and Analysis Organization, or ISAO means any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

- (1) Gathering and analyzing CII in order to better understand security

problems and interdependencies related to critical infrastructure and protected systems in order to ensure the availability, integrity, and reliability thereof;

(2) Communicating or sharing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or to any other entities that may be of assistance in carrying out the purposes specified in this section.

Local Government has the same meaning as is established in section 2 of the Homeland Security Act of 2002 and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a non-profit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in § 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

Protected System means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a fa-

cility of critical infrastructure and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

Purpose of CII has the meaning set forth in section 214(a)(1) of the CII Act of 2002 and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

Submission to DHS as referenced in these procedures means any transmittal of CII to the DHS Protected CII Program Manager or the Protected CII Program Manager's designees, as set forth in § 29.5.

Voluntary or Voluntarily, when used in reference to any submission of CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information; such submission may be accomplished by (*i.e.*, come from) a single entity or by an ISAO acting on behalf of its members. In the case of any action brought under the securities laws—as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—the term “voluntary” does not include information or statements contained in any documents or materials filed, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(i)), with the Securities and Exchange Commission or with Federal banking regulators; and with respect to the submission of CII, it does not include any disclosure or writing that when made accompanies the solicitation of an offer or a sale of securities. The term also explicitly excludes information or statements submitted during a regulatory proceeding or relied upon as a basis for making licensing or permitting determinations.

§ 29.3 Effect of provisions.

(a) *Mandatory submissions of information.* The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information